



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,438	07/08/2003	Patricia Ann Jakubik	RSW920030078US1	7454
25259	7590	04/05/2007		
IBM CORPORATION 3039 CORNWALLIS RD. DEPT. T81 / B503, PO BOX 12195 REASEARCH TRIANGLE PARK, NC 27709			EXAMINER FRINK, JOHN MOORE	
			ART UNIT	PAPER NUMBER
			2142	
SHORTENED STATUTORY PERIOD OF RESPONSE		NOTIFICATION DATE	DELIVERY MODE	
3 MONTHS		04/05/2007	ELECTRONIC	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/05/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

RSWIPLAW@us.ibm.com

Office Action Summary	Application No. 10/615,438	Applicant(s) JAKUBIK ET AL.	
	Examiner John M. Frink	Art Unit 2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☒ Claim(s) 3, 6 and 7 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. ____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>10/17/2003</u> . | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Claim Objections

1. Claims 3, 6 and 7 are objected to because of the following informalities: Claim 3 reads 'that is executed at a specified *intervals*', Claim 6 ends with '*when is declared over*' and Claim 7, e) states 'the most frequent *discard discard* type'. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1 – 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Milo et al. (US 2003/0037141 A1) in view of Brendel (US 2005/0125195 A1).

4. Regarding claim 1, Milo et al. show a method of detecting a denial of service attack at a network server, comprising the steps of counting the number of inbound packets and the number of discarded packets X in a specified interval (Fig.1, [0033-0040]), if the number of discarded packets X in the interval exceeds a specified minimum X(MIN) ([0040-0043]), and setting a denial of service event marker when a specified minimum is reached ([0040-0046]).

Milo et al. do not show calculating the percentage of discarded packets.

Brendel shows calculating the percentage of discarded packets ([0023-0025, 0061-0083, 0096]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Milo et al. with that of Brendel in order to utilize a method of determining that a Denial of Service attack is occurring that considers additional information when making its determination and thus may make a more accurate determination.

5. Regarding claim 2, Milo et al. in view of Brendel further show collecting relevant inbound packet information to further characterize the attack (Milo et al., [0035-0036,0040-0043]).

6. Regarding claim 3, Milo et al. in view of Brendel further show initiating a flood monitoring process that is executed at specified intervals to collect the relevant inbound packet information while the attack is in progress (Brendel [005-0056,0023-0025]).

7. Regarding claim 4, Milo et al. in view of Brendel further show resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the process is lower than a specified minimum $X(\text{MIN}2)$, wherein $X(\text{MIN}2)$ may or may not equal $X(\text{MIN})$ (Brendel [005-0056], also Milo et al., [0039-0046]).

8. Regarding claim 5, Milo et al. in view of Brendel further show resetting the denial of service event marker if the rate of discarded packets in the specified interval before execution of the process is less than a specified threshold (Brendel [0055-0056]).

9. Regarding claim 6, Milo et al. in view of Brendel further show collecting relevant inbound packet information to further characterize the attack when is declared over (Brendel [0055-0056,0061-0063]).

10. Regarding claim 7, Milo et al. in view of Brendel further show where the collected packet information can consist of one or more of the following: the number of inbound packets in the last interval (Milo et al., Fig.1, [0035-0040]); the number of discarded packets in the last interval (Milo et al., Fig.1, [0035-0040]); and the most frequent discard type (Milo et al., Fig.1, [0035-0040]).

11. Regarding claim 8, Milo et al. in view of Brendel further show determining if the flood attack is still in progress by comparing the packets discarded in the last interval with the number of inbound packets, and maintaining the scheduling of the flood monitoring process if the attack is still in progress (Milo et al., Fig.1, [0035-0040]).

12. Regarding claim 9, Milo et al. in view of Brendel further show collecting relevant inbound packet information for the last interval (Brendel [005-0056,0062-0081]).

13. Claims 1, 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Milo et al. in view of Levay et al. (US 6,480,892 B1).

14. Regarding claim 1, Milo et al. show a method of detecting a denial of service attack at a network server, comprising the steps of counting the number of inbound packets and the number of discarded packets X in a specified interval (Fig.1, [0033-0040]), if the number of discarded packets X in the interval exceeds a specified minimum X(MIN) ([0040-0043]), and setting a denial of service event marker when a specified minimum is reached ([0040-0046]).

Milo et al. do not show calculating the percentage of discarded packets.

Levay et al. show calculating the percentage of discarded packets (Fig. 7, col. 15 lines 15 – 23).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the disclosure of Milo et al. with that of Levay et al. in order to utilize a method of determining that a Denial of Service attack is occurring that considers additional information when making its determination and thus may make a more accurate determination.

15. Regarding claim 2, Milo et al. in view of Levay et al. further show collecting relevant inbound packet information to further characterize the attack (Milo et al., [0035-0036,0040-0043]).

16. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Milo et al. in view of Levay et al. as applied to claims 1 and 2 above, and further in view of Swander (US 6,904,529 B1).

17. Regarding claim 3, Milo et al. in view of Levay et al. show the method of claim 1.

Milo et al. in view of Levay et al. do not show initiating a flood monitoring process that is executed at a specified intervals to collect the relevant inbound packet information while the attack is in progress.

Swander shows initiating a flood monitoring process that is executed at a specified interval to collect the relevant inbound packet information while the attack is in progress (col. 6 line 28 – col. 8 line 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the disclosure of Milo et al. in view of Levay et al. with that of Swander et al. in order to continue to gather information regarding a Denial of Service

Art Unit: 2142

attack in order to better understand the methods of the attacker and the attacks effects so that it may be better prevented and/or managed in the future.

18. Regarding claim 4, Milo et al. in view of Levay et al. and Swander further show resetting the denial of service event marker if the number of discarded packets in the specified interval before execution of the process is lower than a specified minimum $X(\text{MIN}2)$, wherein $X(\text{MIN}2)$ may or may not equal $X(\text{MIN})$ (Swander, Fig. 3 and col. 6 line 26 – col. 8 line 3).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John M. Frink whose telephone number is (571) 272-9686. The examiner can normally be reached on M-F 7:30AM - 5:00PM EST; off alternate Fridays.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571)272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2142

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

John Frink

(571) 272-9686


ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER